UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION

KENNETH C. GRIFFIN, Plaintiff, v. INTERNAL REVENUE SERVICE and U.S. DEPARTMENT OF THE TREASURY, Defendants.	Case No. 1:22-cv-24023-Scola/Goodman **Jury Trial Demanded**

AMENDED COMPLAINT

For years, the Internal Revenue Service ("IRS") and the U.S. Department of Treasury (collectively, "Defendants") have been warned by congressional committees, the Treasury Inspector General for Tax Administration ("TIGTA"), and the U.S. Government Accountability Office ("GAO") of their repeated failures to adequately establish appropriate administrative, technical, and physical safeguards over their records systems to protect the sensitive, private, and confidential tax return information they receive from American taxpayers year after year. After flouting these warnings for over a decade, from as early as 2018 to at least 2021, IRS employee[1] Charles "Chaz" Littlejohn ("Mr. Littlejohn"), likely together with other IRS employees, exploited those failures. Indeed, on October 12, 2023, Mr. Littlejohn pled guilty to a violation of 26 U.S.C.

[1] The IRS's Internal Revenue Manual ("IRM") defines "[e]mployee" as "all IRS personnel" including "all contractors who have staff-like access." *See IRS Unauthorized Access, Attempted Access, Or Inspection of Taxpayer Records ("UNAX") Program Policy, Guidance, and Requirements ("UNAX Policy")*, IRM § 10.5.5.1.6(2). According to the IRS, "staff-like access" means "when a contracted individual is granted access to IRS facilities or IRS systems, or has opportunity to be exposed to IRS information." *See id.* § 10.5.5.1.6(3).

§ 7213(a)(1) for unlawful disclosure of confidential tax return information and admitted that, while working for the IRS, Defendants provided him access to "IRS data associated with thousands of the nation's wealthiest people, including returns and return information dating back over 15 years," and then he used that access to unlawfully inspect and repeatedly disclose confidential tax return information to various media outlets. The confidential tax return information that Mr. Littlejohn unlawfully inspected and disclosed included the private information of Plaintiff Kenneth C. Griffin ("Mr. Griffin").

Accordingly, Mr. Griffin, by and through his undersigned counsel, brings this action against the IRS and the U.S. Department of Treasury to seek redress for the IRS's unlawful inspections and disclosures of Mr. Griffin's confidential tax return information in violation of 26 U.S.C. § 6103 as well as Defendants' violation of the Privacy Act, 5 U.S.C. § 552a, for their willful and intentional failure to establish appropriate administrative, technical, and/or physical safeguards over their records system to insure the security and confidentiality of Mr. Griffin's confidential tax return information.

INTRODUCTION

1. Mr. Griffin, a self-made entrepreneur and investor, is the founder and Chief Executive Officer of Citadel, a global alternative investment firm, and a founder and the non-Executive Chairman of Citadel Securities, a leading global market maker. He is proud of his success and has always sought to pay his fair share of taxes. Indeed, Mr. Griffin apparently pays federal income taxes at a higher effective tax rate than many of the top wage earners in the United States.[2]

[2] ProPublica, *America's Top 15 Earners and What They Reveal About the U.S. Tax System*, PROPUBLICA, April 13, 2022, https://www.propublica.org/article/americas-top-15-earners-and-what-they-reveal-about-the-us-tax-system.

2. Mr. Griffin has complied with the IRS's annual requirements to report his personal and confidential financial information, and he did so—like virtually all Americans—believing that the IRS would comply with its own legal obligations to safeguard and protect his information from unauthorized inspection and disclosure, as required by Section 6103 of the Internal Revenue Code as well as the Privacy Act, 5 U.S.C. § 552a. It did not.

3. Instead, from as early as 2018 through at least 2020, IRS personnel (including Mr. Littlejohn) violated 26 U.S.C. § 6103 by exploiting the IRS's willful failure to establish adequate administrative, technical, and physical safeguards for the IRS's data and records systems to: 1) repeatedly and unlawfully inspect and misappropriate confidential tax return information for the highest earning U.S. taxpayers, including Mr. Griffin; and 2) unlawfully disclose those materials to ProPublica for publication.

4. For example, in or around September 2020, Mr. Littlejohn contacted and discussed with ProPublica the possibility of giving the media outlet a copy of the confidential tax return information of thousands of the nation's wealthiest people, covering more than 15 years, including the confidential tax return information that Mr. Griffin reported to the IRS. Then, from September 2020 through November 2020, Mr. Littlejohn—enabled by the systemic IRS security failures described above and in more detail below—unlawfully disclosed this information to ProPublica in violation of 26 U.S.C. § 6103. ProPublica went on to boast that the information it obtained was "not just tax returns," but also included "information that is sent to the IRS about financial activities" such as "income and taxes," "investments, stock trades, gambling winnings and even the results of audits."[3] Significantly, ProPublica identified the IRS as the source of the

[3] ProPublica, *The Inside Story of How We Reported the Secret IRS Files*, PROPUBLICA, August 6, 2021, https://www.propublica.org/article/the-inside-story-of-how-we-reported-the-secret-irs-files.

confidential information it published, including Mr. Griffin's return information.

5. In or around March 2022, Mr. Griffin came to know about the IRS's unlawful disclosures and violations of the Privacy Act when he learned that ProPublica intended to publish a story "about the highest earning Americans, in which [ProPublica] plan[ned] to mention several dozen people including [Mr.] Griffin," as well as another story contrasting the relatively high effective income tax rate that Mr. Griffin pays with the apparently lower effective tax rate paid by the CEO of one of Citadel Securities' commercial competitors.

6. On April 13, 2022 and on July 7, 2022, ProPublica published confidential tax return information regarding Mr. Griffin's 2013-2018 federal income tax years, including Mr. Griffin's purported average annual income, purported percent of income deducted, and purported average effective federal income tax rate for those periods.[4] In publishing the information, ProPublica acknowledged that it was the confidential tax return information of "people who, in good faith, sent their tax and personal and private information to the Internal Revenue Service with no expectation that it would ever be made public."[5]

7. To date, ProPublica has published nearly 50 articles using the tax returns and confidential tax return information Mr. Littlejohn provided to ProPublica. It is clear why Mr. Griffin's and these other taxpayers' confidential tax return information was and continues to be so readily available to ProPublica: the IRS's well-known, systemic failures to establish

[4] Paul Kiel & Mick Dumke, *Ken Griffin Spent $54 Million Fighting a Tax Increase for the Rich. Secret IRS Data Shows It Paid Off for Him*, PROPUBLICA, June 7, 2022, https://www.propublica.org/article/ken-griffin-illinois-graduated-income-tax; ProPublica, *America's Top 15 Earners and What They Reveal About the U.S. Tax System*, PROPUBLICA, April 13, 2022, https://www.propublica.org/article/americas-top-15-earners-and-what-they-reveal-about-the-us-tax-system.

[5] ProPublica, *The Inside Story of How We Reported the Secret IRS Files*, PROPUBLICA, August 6, 2021, https://www.propublica.org/article/the-inside-story-of-how-we-reported-the-secret-irs-files.

appropriate safeguards to protect taxpayers' confidential return information from unauthorized and unlawful inspection and disclosure.

8. Federal agencies depend on information technology systems and electronic data to carry out operations and to process, maintain, and report essential information. Every year from fiscal year 2010 through 2020, however, TIGTA has put the IRS on notice that deficiencies in its "Security Over Taxpayer Data and Protection of IRS Resources" were the IRS's "number one major management and performance challenge area."[6]

9. Despite annual audits, TIGTA—for more than a decade—continued to find systemic failures by the IRS to establish appropriate administrative, technical, and physical safeguards to adequately protect against the unlawful disclosure of taxpayers' confidential tax return information. For example, in its *Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2020*, TIGTA revealed that the IRS failed to use "encryption algorithms" in accordance with the Federal Processing Standards 140-2, *Security Requirements for Cryptographic Modules* for certain operating systems in order to keep confidential tax return information "unreadable for an unauthorized user."[7] Likewise, TIGTA reported that 2 out of 5 of the IRS's Cybersecurity Framework functions (*i.e.*, Identify, Protect, Detect, Respond, Recover) "were deemed as 'not effective.'"[8] TIGTA also identified myriad security deficiencies for the IRS system that collects, converts, and stores a taxpayer's confidential tax return information into

[6] *See* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2021-20-001, ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE'S INFORMATION TECHNOLOGY PROGRAM FOR FISCAL YEAR 2020, at 6 (October 2020).

[7] *See id.* at 22.

[8] *See id.* at 9.

electronic records of taxpayer data,[9] including "more than 16,000 policy violations."[10] In other instances, "the IRS inappropriately assigned business role accounts to an administrator group, resulting in those accounts [and thus inappropriate employees] having unnecessary elevated privileges."[11] Notably, TIGTA found that the IRS "lacked management oversight to ensure that Federal and [Internal Revenue Manual] requirements are met" and, in "critical areas" housing computer rooms, "the IRS cannot control the movement of individuals and eliminate unnecessary traffic throughout this critical security area [to] reduce the opportunity for unauthorized disclosure or theft of tax information."[12]

10. The IRS is and has for some time been well aware of these data security failures, including the unlawful disclosure of Mr. Griffin's confidential tax return information at issue in this lawsuit. Presciently, on April 18, 2022, more than a year before Mr. Littlejohn was criminally charged, members of Congress confirmed that there "is little doubt" that the confidential tax return information disclosed to ProPublica, including Mr. Griffin's confidential tax return information, "came from inside the IRS" and that the disclosure was "precisely what 26 U.S.C. § 6103 and related statutes were designed to prevent—the disclosure of private tax information and the political weaponization of that information."[13]

---

[9] TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2020-20-006, ACTIVE DIRECTORY OVERSIGHT NEEDS IMPROVEMENT, at 1-2 (February 2020).

[10] *Id.* at *Highlights.*

[11] *Id.*

[12] *Id.* at 6.

[13] Letter from Congressman Kevin Brady and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (April 18, 2022), https://gop-waysandmeans.house.gov/wp-content/uploads/2022/04/4-18-2022-Brady-Crapo-to-Yellen_FINAL.pdf.

11. Despite these warnings and clearly illegal disclosures to ProPublica, however, the IRS continued—and on information and belief, continues—to willfully and intentionally fail to establish adequate safeguards to protect Mr. Griffin's and other taxpayers' confidential tax return information. For example, "the IRS continues cloud deployments [that contain taxpayer data] despite not having a fully implemented security control infrastructure in place."[14] In so doing, the "IRS implemented cloud services with known capability gaps that remain in the areas of identity and access management, continuous security monitoring, data and infrastructure protection, and program management and integration."[15] In other instances, even when the IRS agreed with TIGTA recommendations to take corrective actions and perform database vulnerability scanning enterprise-wide by 2016, "the IRS made an executive decision, without following proper procedures or policy, to reduce vulnerability scanning of databases."[16] What is more, the IRS concealed its decision until TIGTA started a review in November 2020, at which time "the IRS officially announced the reduction in database vulnerability scanning, three years after it had actually reduced database vulnerability scanning."[17] Although computer mainframes are considered High Value Assets, the "IRS has not performed database vulnerability scanning on [its]

[14] TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2022-20-052, CLOUD SERVICES WERE IMPLEMENTED WITHOUT KEY SECURITY CONTROLS, PLACING TAXPAYER DATA AT RISK, at *Highlights* (September 27, 2022).

[15] *Id.* at 6.

[16] TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2022-20-065, THE IRS NEEDS TO IMPROVE ITS DATABASE VULNERABILITY SCANNING AND PATCHING CONTROLS, at *Highlights*, 3 (September 30, 2022).

[17] *Id.* at 4.

International Business Machines (IBM) mainframes since 2018,"[18] and according to TIGTA, "the IRS is not timely patching database vulnerabilities."[19]

12. The IRS also failed to meet its obligations by failing to establish safeguards that included "centralized oversight of contractor [data security] training."[20] And, despite this identified gap in data security, the IRS "has not conducted an initial risk assessment to identify whether its method of sharing the data electronically [with contractors] appropriately protects taxpayer information,"[21] nor does the IRS "have a supplemental policy or guidance that requires a risk assessment to be performed prior to transferring taxpayer information to contractors."[22]

13. These pervasive data security failures, and the refusal by IRS employees to correct these failures, allowed Mr. Littlejohn to repeatedly inspect and then misappropriate the confidential tax return information of thousands of the nation's wealthiest taxpayers, including Mr. Griffin; upload that data to a private website; and then disclose that return information to ProPublica in or about November 2020.

14. Since ProPublica began using the confidential tax return information of thousands of taxpayers that it received from the IRS, members of Congress have repeatedly demanded to know how the IRS and the Treasury Department could have allowed these unlawful disclosures to

[18] *Id.* at 4-6.

[19] *Id.* at *Highlights*.

[20] *See* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, GAO-23-105395, SECURITY OF TAXPAYER INFORMATION, IRS NEEDS TO ADDRESS CRITICAL SAFEGUARD WEAKNESSES, at 31 (August 2023).

[21] *See id.* at 52.

[22] *See id*.

happen.[23] Members of the House Ways and Means Committee sent letters on June 9, 2021, June 11, 2021, June 17, 2021, April 18, 2022, and October 27, 2022 to Treasury Secretary Janet Yellen, IRS Commissioner Charles Rettig, Treasury Inspector General for Tax Administration J. Russell George, and Acting Inspector General for the U.S. Department of Treasury Richard Delmar, and also asked questions at hearings on June 17, 2021 and June 8, 2022, to obtain information "about the actions that led to the massive leak of private taxpayer information in June 2021 to ProPublica."[24] Likewise, Mr. Griffin repeatedly requested that Defendants provide him information relevant to the unlawful disclosure of his own confidential tax return information to ProPublica, and demanded that Defendants "send a formal demand to ProPublica to return (and destroy any copies therewith) all of the confidential IRS data ProPublica has in its possession, custody, or control."

15. Defendants responded to both Congress and Mr. Griffin with brazen stonewalling. It was not until September 29, 2023—more than two years after ProPublica began publishing articles with the confidential return information it received from the IRS and nearly a year after Mr. Griffin filed his initial complaint in this action—when the United States finally charged Mr. Littlejohn and at least some information was made public.[25] Even then, despite

---

[23] *See, e.g.*, Letter from Congressman Kevin Brady and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (April 18, 2022), https://gop-waysandmeans.house.gov/wp-content/uploads/2022/04/4-18-2022-Brady-Crapo-to-Yellen_FINAL.pdf; *see also The Financial Stability Oversight Council Annual Report to Congress: Hearing Before the S. Banking Comm.* (May 10, 2022), https://www.youtube.com/watch?v=_ObS-QV0OEw, at approximately 1:29.

[24] *See* Letter from Congresspeople Kevin Brady, Jodey Arrington, and David Kustoff to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (October 27, 2022), https://gop-waysandmeans.house.gov/wp-content/uploads/2022/10/10.27.22-ProPublica-Leak-Letter.pdf.

[25] In fact, Defendants' initial motion to dismiss—before falling moot following the announcement of the criminal charges against Littlejohn—was premised in large part on the

publicly charging one of Defendants' employees in connection with the scheme to expose Mr. Griffin's confidential information, Defendants are continuing to double-down on their stonewalling of Mr. Griffin. Among other things, Defendants refuse to provide Mr. Griffin with any additional information concerning the obvious connection between the unlawful inspections and disclosures of his confidential tax return information to ProPublica and the well-documented failures of the IRS to take seriously its obligations to establish appropriate safeguards to protect the confidential tax return information of United States taxpayers. Nor has the IRS provided any concrete assurance by specifying anything it is doing to prevent these harmful breaches from recurring.

16. In enacting 26 U.S.C. §§ 6103 and 7431, as well as 5 U.S.C. § 552a(e)(10), Congress unequivocally declared its intent to safeguard the confidentiality of U.S. taxpayers' tax return information, including Mr. Griffin's confidential tax return information, and to hold the IRS to account for failing to adequately do so. By this lawsuit, Mr. Griffin respectfully requests that the Court provide damages and injunctive relief to enforce Congress's promise.

JURISDICTION AND VENUE

17. This Court has jurisdiction pursuant to 28 U.S.C. §§ 1331, 1340, 1346, 26 U.S.C. § 7431(a), and 5 U.S.C. § 552a(g)(1)(D).

18. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1402 because Mr. Griffin resides in this judicial district.

---

argument that Defendants could not ascertain how Mr. Griffin's tax records had been disclosed to ProPublica or who had disclosed them.

THE PARTIES[26]

19. Plaintiff Kenneth C. Griffin is a citizen of the United States and a resident of Miami, Florida.

20. Defendant U.S. Department of the Treasury is an Executive Department of the United States of America and oversees the IRS and TIGTA.

21. Defendant Internal Revenue Service is a bureau of the U.S. Department of the Treasury and is responsible for the administration and enforcement of the Internal Revenue Code.

22. Charles Edward Littlejohn is a person who has held himself out to be a Data Process Management employee of the IRS from July 2012 through the present. Upon information and belief, Mr. Littlejohn either worked directly for the IRS or worked as an IRS contractor from 2008 through 2021, including specifically from 2008 to 2010, from 2012 to 2013, and from 2017 to 2021.

23. At all relevant times, Mr. Littlejohn was an officer or employee of the United States by virtue of his employment with or for the IRS,[27] because he had staff-like access to returns and confidential tax return information,[28] because he held himself out to the public as an employee of the IRS from 2012 through the present, because he was a member of a group for which only IRS employees are allowed membership,[29] and because Defendants had and exercised the power to

---

[26] Defendants, as the United States, are proper party defendants in this action and have waived sovereign immunity pursuant to 26 U.S.C. § 7431 and 5 U.S.C. § 552a(g)(1)(D).

[27] *See supra,* n.1; *see also*, *e.g.,* IRM § 7.11.13.1.1(3) ("All IRS employees (including managers, executives *and contractors*) are responsible for protecting the confidentiality and privacy of taxpayer information to which they have access.") (emphasis added).

[28] Mr. Littlejohn falls squarely within the IRM's definition of "[e]mployee" because he had staff-like access to IRS facilities and IRS systems. *See supra*, n.1.

[29] Mr. Littlejohn is a member of the Internal Revenue Service (IRS) [unofficial] group on LinkedIn, which "is established to connect only present employees across various segments and

control the detailed physical performance of Mr. Littlejohn's work.

24. Indeed, the IRS (including IRS Contracting Officer Representatives)[30] exercised extensive, detailed, day-to-day supervision of Mr. Littlejohn's work, particularly at IRS facilities and with IRS data systems, and by, among other things: managing the scope and purpose of Mr. Littlejohn's daily tasks and projects; ensuring that Mr. Littlejohn completed required training, monitoring Mr. Littlejohn's technical performance; ensuring Mr. Littlejohn was aware of data safeguards and appropriately protecting taxpayer information; and exercising control over the parameters of Mr. Littlejohn's access to IRS data and confidential tax return information, including Mr. Griffin's confidential tax return information. Moreover, the IRS also had authority to reprimand and/or terminate Mr. Littlejohn. According to the IRS, all IRS employees—*i.e.*, "all IRS personnel," which "[a]lso includes all contractors who have staff-like access"[31]—"may be subject to administrative penalties for the willful and unauthorized attempted access of their own or another taxpayer's records."[32] IRS administrative penalties include, but are not limited to, removal of employees and suspension of employees.

service centers" and "note[s] that all LinkedIn profiles will be checked prior to approval into the IRS group." *See* https://www.linkedin.com/in/charles-littlejohn-710bb660/; and https://www.linkedin.com/groups/156949/.

[30] Contracting Officer Representatives are "IRS employees who oversee day-to-day operations of contracts and contractors." *See* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, GAO-23-105395, SECURITY OF TAXPAYER INFORMATION, IRS NEEDS TO ADDRESS CRITICAL SAFEGUARD WEAKNESSES, at 35 (August 2023).

[31] *See* IRM § 10.5.5.1.6(2) and (3).

[32] IRM § 10.5.5.2(2).

FACTUAL ALLEGATIONS

I. The IRS Willfully Failed To Establish Appropriate Administrative, Technical, And Physical Safeguards To Insure The Security And Confidentiality Of Mr. Griffin's Confidential Tax Return Information.

25. The IRS relies extensively on computerized systems of records to support its financial and mission-related operations. The IRS knows and has known that without effective security controls, the IRS's systems of records are vulnerable to, among other things, malicious efforts by IRS employees or contractors to illicitly obtain and misappropriate confidential taxpayer information.

26. As detailed above, however, TIGTA has put the IRS on notice for a decade that deficiencies in its "Security Over Taxpayer Data and Protection of IRS Resources" were the agency's "number one major management and performance challenge area."[33] Despite being aware of its security deficiencies for over a decade, the IRS willfully failed to establish appropriate administrative, technical, and physical safeguards to insure the security of confidential tax return information, including Mr. Griffin's confidential tax return information.

27. For example, the IRS uses Microsoft Active Directory ("Microsoft AD") services for its data security systems, including to facilitate secure user logon, access authorization, and credentialed validation for Windows laptops, desktops, and servers for all IRS employees, contractors, and business applications that interact with these computers.[34] The IRS is also supposed to use Microsoft AD to enforce the Internal Revenue Manual and operational standards

---

[33] *SEE* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2021-20-001, ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE'S INFORMATION TECHNOLOGY PROGRAM FOR FISCAL YEAR 2020, at 6 (October 2020).

[34] *See* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2018-20-034, ACTIVE DIRECTORY OVERSIGHT NEEDS IMPROVEMENT AND CRIMINAL INVESTIGATION COMPUTER ROOMS LACK MINIMUM SECURITY CONTROLS, at 1 (June 2018).

for all Windows laptops, desktops, servers, user accounts, and service accounts.[35] In short, the IRS is supposed to use Microsoft AD to establish appropriate administrative, technical, and physical safeguards to protect Mr. Griffin's confidential taxpayer information by, among other things, centralizing management of computers and users for data security purposes.[36]

28. In September 2011, over a decade ago, TIGTA reported that "the IRS did not enforce the centralization of its Windows environment," thus failing to establish safeguards to "achieve[] consistent identity and authentication management, [as] required by Federal regulations and IRS enterprise architecture security principles."[37] The IRS also "did not ensure that all Windows computers connected to its network were authorized and compliant with security policy, putting the IRS at risk of security breaches."[38] And, although the IRS created standards to prevent unauthorized computers from being connected to the network, "it had not established a central controlling authority to enforce compliance with its policy."[39] In response, TIGTA recommended that the IRS establish a governing body that would, among other things, finalize and enforce security design criteria, develop standards, and ensure that unauthorized data systems are not implemented.[40]

29. Seven years later, in 2018, after auditing the IRS's implementation of TIGTA's recommendation to establish certain technical and physical data security safeguards, TIGTA

---

[35] *Id.*

[36] *Id.*

[37] *Id.* (citing TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2011-20-111, CONTINUED CENTRALIZATION OF THE WINDOWS ENVIRONMENT WOULD IMPROVE ADMINISTRATION AND SECURITY EFFICIENCIES (Sept. 2011)).

[38] Report No. 2018-20-034 at 2.

[39] *Id.*

[40] *Id.*

found, among other things, 88 physical security control weaknesses and over 1,700 improperly configured user accounts.[41] TIGTA also found that the IRS's Windows Policy Checker was out of date and used three-year-old technical guidelines to conduct its analysis.[42] As a result, TIGTA concluded "the IRS cannot ensure that sensitive taxpayer information and taxpayer dollars are preserved and protected."[43]

30. The IRS continued its failure to implement appropriate safeguards through at least Fiscal Year 2020. For example, the Federal Information Security Modernization Act of 2014 ("FISMA") required the IRS to establish appropriate administrative, technical, and physical safeguards over its system of records by, among other things, developing, documenting, and implementing an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by contractors. In its *Annual Assessment of the Internal Revenue Service's Information Technology Program for Fiscal Year 2020*, however, TIGTA reported the following IRS failures, among others:

- **40% of the IRS's Cybersecurity Framework Function Areas Were Deemed "Not Effective."**[44] Two out of five Cybersecurity Framework function areas (*i.e.*, Identify, Protect, Detect, Respond, and Recover) were deemed "not effective."[45] Notably, ***the IRS failed to effectively establish the organizational understanding to manage cybersecurity risks*** to systems, assets, and capabilities (*i.e.*, the Identify function) and also failed to effectively establish and implement the appropriate activities to identify the occurrence of a cybersecurity event (*i.e.*, the Detect function).

[41] *Id.* at *Highlights.*

[42] *Id*.

[43] *Id.* at 5.

[44] *See* Report No. 2021-20-001, at 7-9.

[45] *Id.* at 9.

- **Numerous Physical Security Violations in FY2020.**[46] The IRS is aware that physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. In Fiscal Year 2020, TIGTA performed site visits at six IRS locations to evaluate the physical security controls protecting the computer rooms housing the systems that collect, convert, and store a taxpayer's confidential tax return information into electronic records of taxpayer data. Among other violations, TIGTA found six ***violations of the Limited Access policies*** in three of the six locations visited, where visitors and employees with access to larger processing areas also had "***uncontrolled access to the computer room***" that housed these data systems. Moreover, TIGTA also found "***multifactor authentication has not been implemented, as required***, for any of the Limited Area computer rooms in the six locations audited."

- **Access Management – 16,000 Account Policy Violations.**[47] Access management processes help to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify them. In Fiscal Year 2020, TIGTA performed two audits covering the IRS's access management systems over 16,000 violations of the Internal Revenue Manual 10.8.1, *Information Technology (IT) Security – Policy and Guidance* requirements. Notably, TIGTA's audit of controls to authenticate third-party authorization requests revealed that ***54% of the employees audited had unneeded access privileges to the IRS Centralized Authorization File***—*i.e.*, the computerized system of records which houses authorization information from both powers of attorney and tax information authorizations. Of the 54% of unauthorized users, 31% of them initiated actions to modify Centralized Authorization File authorizations between January 2, 2020 and February 29, 2020, despite these employees having jobs such as mail clerks, file supervisors, facility management, or computer assistant, none of which require them to change or add taxpayer authorizations to the Centralized Authorization File system.

- **Failure to Implement Encryption Algorithms.**[48] The IRS is supposed to use cryptography—*i.e.*, encryption algorithms that convert data into a format that is unreadable for unauthorized users—allowing confidential information to be transmitted or stored without unauthorized entities decoding it back into a readable format. In Fiscal Year 2020, the Government Accountability Office ("GAO") performed an audit of the IRS's information system security controls and found that the ***IRS failed to establish and implement cryptographic mechanisms to secure data in IRS systems*** that process taxpayer data. The GAO also found that the IRS failed to enforce the use of encryption algorithms

[46] *Id.* at 13-14.

[47] *Id.* at 21-22.

[48] *Id.* at 22.

as required by the Federal Information Processing Standards 140-2, *Security Requirements for Cryptographic Modules* for certain operating systems.

31. Similarly, TIGTA has found that the IRS failed to establish safeguards allowing the IRS to even *detect*, much less prevent, unauthorized access to confidential tax return information. Indeed, on July 31, 2020, TIGTA revealed that "the IRS could not provide an accurate inventory of all applications that store or process taxpayer data and [Personally Identifiable Information]."[49] In fact, 91% of monitored applications provided either "incomplete and inaccurate audit trails" or "no audit trails" at all.[50] Likewise, on September 14, 2022, TIGTA reported that the IRS's "current [physical security] processes do not ensure that recommended minimum security countermeasures are tracked and considered,"[51] particularly "because the IRS does not consistently use a centralized system to track physical security countermeasures, recommendations, approvals, implementation actions, and associated costs."[52]

32. Apparently untroubled by these data security failures, the IRS put and continues to put Mr. Griffin's and other United States taxpayers' confidential tax return information at risk. The IRS's policies and procedures require that IRS employees, including contractor-employees such as Mr. Littlejohn, complete annual IRS-provided data security training before giving them

---

[49] *See* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2020-20-033, MOST INTERNAL REVENUE SERVICE APPLICATIONS DO NOT HAVE SUFFICIENT AUDIT TRAILS TO DETECT UNAUTHORIZED ACCESS TO SENSITIVE INFORMATION, at 2 (July 31, 2020).

[50] *Id.* at *Highlights*, 2.

[51] TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2022-10-046, THE PROCESS FOR TRACKING PHYSICAL SECURITY WEAKNESSES IDENTIFIED IN IRS FACILITIES DOES NOT ENSURE THAT VULNERABILITIES ARE PROPERLY ADDRESSED, at 6 (September 14, 2022) (cleaned up).

[52] *Id.* at *Highlights*.

access to confidential tax return information.[53] The IRS is also required to monitor and remove access to confidential tax return information if they do not keep up to date with the required annual training.[54] Despite these requirements, however, a recent report by the GAO that "evaluate[d] the extent to which [the] IRS is following its tax safeguards for protecting taxpayer information"[55] found that the IRS failed to establish "centralized oversight of contractor [UNAX and data security] training,"[56] and thus, the "IRS has no measure to use to assess contractor training completion rates."[57] Based on the GAO's analysis, most of the UNAX and data security training modules it audited had a completion rate among contractors between 61% to 69% for fiscal year 2021, and none of them had a completion rate among contractors over 74%.[58] Accordingly, on information and belief, the IRS has habitually violated its own policies and procedures by providing IRS personnel (including Mr. Littlejohn[59]) access to confidential tax return information regardless of whether they complete or remain up to date with all of the required annual privacy and data security training.

---

[53] *See* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, GAO-23-105395, SECURITY OF TAXPAYER INFORMATION, IRS NEEDS TO ADDRESS CRITICAL SAFEGUARD WEAKNESSES, at 30-31 (August 2023).

[54] *See id.*

[55] *Id.* at 3.

[56] *Id.* at 31.

[57] *Id.* at 32.

[58] *Id.* at 30, Table 3.

[59] Consistent with the inexcusably low completion rates of UNAX and data security training among IRS personnel that the GAO reported, the Factual Basis for Mr. Littlejohn's plea agreement also suggests that he did not receive *all* of the data security training required by the IRS's policies and procedures, particularly as the Factual Basis notes that Mr. Littlejohn only received "regular" (but not all of the required) training about protecting taxpayer data over the course of his employment with the IRS between 2008 and 2021. *See United States v. Charles Edward Littlejohn*, 1:23-cr-00343-ACR ECF 9 ¶ 4 (D.D.C. Oct. 12, 2023).

33. Separately, the IRS is obligated to develop Plans of Action and Milestones ("POA&M") for IRS systems to document its planned remediation of weaknesses. According to POA&M Standard Operating Procedures, "critical and high-risk vulnerabilities that cannot be remediated within 30 to 60 calendar days should be documented as POA&Ms in the Treasury Department's FISMA Information Management System or the Authorizing Official should pursue a risk-based decision."[60] TIGTA recently sampled 10 FISMA systems from the IRS's database vulnerability scanning tool's report that required POA&Ms, and on September 14, 2022, TIGTA reported that POA&Ms "were not created for database vulnerabilities" and "concluded that the IRS lacked managerial oversight to ensure that it appropriately documented corrective actions."[61] As a result, "the IRS cannot ensure that it is correcting and managing its information security weaknesses […] thereby exposing its systems to increased risk that nefarious actors will exploit the deficiencies to gain unauthorized access to information resources."[62]

34. The IRS's failure to establish appropriate administrative, technical, and physical safeguards over its systems of records has been willful, at the very least, and Mr. Littlejohn exploited these willful failures to repeatedly inspect and misappropriate Mr. Griffin's confidential tax return information and unlawfully disclose that information to ProPublica for further publication.

II. IRS Personnel Repeatedly And Unlawfully Inspected And Unlawfully Disclosed Mr. Griffin's Confidential Tax Return Information.

35. In response to a series of stories that ProPublica published in 2018 regarding how

---

[60] TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2022-20-065, THE IRS NEEDS TO IMPROVE ITS DATABASE VULNERABILITY SCANNING AND PATCHING CONTROLS, at 9 (September 30, 2022).

[61] *Id.*

[62] *Id.*

IRS budget cuts led to "an exodus of revenue agents, the kind of auditors [ProPublica claims] who really understand taxes and looked at corporations and the wealthy in particular,"[63] Mr. Littlejohn exploited the IRS's willful failures to establish adequate administrative, technical, and physical safeguards for the IRS's data and records systems by repeatedly inspecting and misappropriating confidential tax return information for the highest-earning U.S. taxpayers, including Mr. Griffin's confidential tax return information for federal income tax years 2013-2018. Mr. Littlejohn then intentionally and maliciously disclosed those materials to ProPublica for further publication.

36. Specifically, from as early as July 2020 through at least August 2020, on information and belief, Mr. Littlejohn exploited at least the following IRS data security failures—which should have been well-known within the IRS given the repeated and public nature of the reports highlighting those failures—to repeatedly and unlawfully inspect as well as misappropriate Mr. Griffin's and thousands of others' confidential tax return information:

- The IRS's failure to "ensure that all Windows computers connected to its network were authorized and compliant with security policy,"[64] which allowed IRS personnel (including Mr. Littlejohn) to use virtual machines that simulated physical computers to avoid IRS protocols designed to detect and prevent large downloads or uploads from IRS devices or systems;

- The IRS's failure to adequately establish the organizational understanding to manage cybersecurity risks,[65] which allowed Mr. Littlejohn to repeatedly access, inspect, and misappropriate Mr. Griffin's and thousands of other taxpayers' confidential return information without detection by uploading the data to a private website; and

- The IRS's failure to use adequate encryption algorithms that convert data into a format that is unreadable for unauthorized users,[66] which allowed

[63] ProPublica, *The Inside Story of How We Reported the Secret IRS Files*, PROPUBLICA, August 6, 2021, https://www.propublica.org/article/the-inside-story-of-how-we-reported-the-secret-irs-files.

[64] Report No. 2018-20-034 at 2.

[65] *See* Report No. 2021-20-001, at 7-9.

[66] *Id.* at 22.

> Mr. Littlejohn to store and transmit Mr. Griffin's and thousands of other taxpayers' confidential tax return information to ProPublica on a personal data storage device, while also allowing ProPublica to decode the data into a readable format after the unlawful disclosures.

37. In or about September 2020, including Mr. Littlejohn contacted and discussed with ProPublica the possibility of unlawfully disclosing a copy of Mr. Griffin's and thousands of others' confidential tax return information to them. Then, from as early as September 2020 to at least November 2020, Mr. Littlejohn—enabled by the systemic security failures described above—unlawfully disclosed Mr. Griffin's and thousands of others' confidential tax return information to ProPublica on a personally-owned storage device.

38. In or around March 2022, Mr. Griffin learned that ProPublica was in possession of his confidential tax return information, along with the confidential tax return information "of thousands of the nation's wealthiest people, covering more than 15 years."[67] The information ProPublica obtained was "not just tax returns," but also included "information that is sent to the IRS about financial activities" such as "income and taxes," "investments, stock trades, gambling winnings and even the results of audits."[68]

39. ProPublica has published over 50 articles containing the confidential tax return information of the taxpayers targeted by its articles, accompanied by what members of Congress describe as "politicized, misleading and likely inaccurate rhetoric and analysis."[69] For example,

---

[67] Jesse Eisinger, Jeff Ernsthausen & Paul Kiel, *The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax*, PROPUBLICA, June 8, 2021, https://www.propublica.org/article/the-secret-irs-files-trove-of-never-before-seen-records-reveal-how-the-wealthiest-avoid-income-tax.

[68] *Id.*

[69] Letter from Congressman Kevin Bradley and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (April 18, 2022), https://gop-waysandmeans.house.gov/wp-content/uploads/2022/04/4-18-2022-Brady-Crapo-to-Yellen_FINAL.pdf.

on April 13, 2022, ProPublica published confidential tax return information for Mr. Griffin's 2013-2018 federal income tax years, including Mr. Griffin's purported average annual income, purported percent of income deducted, and purported average effective federal income tax rate for those periods.[70] In July 2022, ProPublica again published Mr. Griffin's (and others') confidential tax return information to criticize Mr. Griffin's opposition to Illinois Governor J.B. Pritzker's 2020 referendum to burden hard-working families in Illinois with yet more taxes.[71]

40. Although members of Congress have confirmed that there "is little doubt" that the confidential tax return information disclosed to ProPublica, including Mr. Griffin's confidential tax return information, "does precisely what 26 U.S.C. § 6103 and related statutes were designed to prevent—the disclosure of private tax information and the political weaponization of that information,"[72] it took more than two years before the United States finally brought a criminal charge regarding these unlawful disclosures. And even now, Defendants continue to stonewall Mr. Griffin by refusing to provide him with information regarding the obvious connection between the unlawful inspections and disclosures of his confidential return information to ProPublica and the well-documented failures of the IRS to protect his and thousands of other United States taxpayers' confidential return information.

---

[70] ProPublica, *America's Top 15 Earners and What They Reveal About the U.S. Tax System*, PROPUBLICA, April 13, 2022, https://www.propublica.org/article/americas-top-15-earners-and-what-they-reveal-about-the-us-tax-system.

[71] Paul Kiel & Mick Dumke, *Ken Griffin Spent $54 Million Fighting a Tax Increase for the Rich. Secret IRS Data Shows It Paid Off for Him*, PROPUBLICA, July 7, 2022, https://www.propublica.org/article/ken-griffin-illinois-graduated-income-tax.

[72] Letter from Congressman Kevin Bradley and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury, dated April 18, 2022.

COUNT I

Violations of 26 U.S.C. § 6103 – Willful or Grossly Negligent Unauthorized Disclosure

41. Mr. Griffin realleges and incorporates by reference each of the preceding paragraphs as if fully set forth herein.

42. Title 26, U.S.C. § 6103 provides that tax "[r]eturns and return information shall be confidential" and prohibits disclosure and inspection by United States employees and other defined persons, except as specifically authorized in the provision.

43. The Internal Revenue Manual § 10.5.5.1.6(2) defines "[e]mployee" as "all IRS personnel" including "all contractors who have staff-like access."

44. The Internal Revenue Manual § 10.5.5.1.6(3) defines "staff-like access" to mean "when a contracted individual is granted access to IRS facilities or IRS systems, or has opportunity to be exposed to IRS information."

45. Title 26, U.S.C. § 6103(n) permits the disclosure of returns and return information to any person "to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration."

46. Title 26, C.F.R. § 301.6103(n)-1(b)(2), however, prohibits such disclosures under 26 U.S.C. § 6103(n) if the disclosure is not "necessary" or, in the alternative, if the services for which the disclosure is made pursuant to 26 U.S.C. § 6103(n) can be "reasonably, properly, or economically performed by disclosure of only parts or portions of a return or if deletion of taxpayer identity information […] reflected on a return would not seriously impair the ability of the employees to perform the service, then only the parts or portions of the return, or only the return with taxpayer identity information deleted, may be disclosed."

47. Title 26, U.S.C. § 7431 provides taxpayers a private right of action for damages against the United States for the knowing or negligent unauthorized inspection or disclosure of tax return information in violation of 26 U.S.C. § 6103.

48. "Return" is defined as "any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed."[73]

49. "Return information" includes "a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense."[74]

50. "[D]isclosure" means "the making known to any person in any manner whatever a return or return information."[75]

51. As alleged herein, the IRS, in part through its employee, Mr. Littlejohn, repeatedly violated 26 U.S.C. § 6103 from as early as July 2020 through at least November 2020 by

[73] 26 U.S.C. § 6103(b)(1).

[74] 26 U.S.C. § 6103(b)(2)(A).

[75] 26 U.S.C. § 6103(b)(8).

unlawfully inspecting Mr. Griffin's confidential tax return information for at least his federal income tax years 2013-2018, and then unlawfully disclosing that information to ProPublica. Those unlawful inspections and disclosures encompassed Mr. Griffin's wage information, charitable contributions, financial and securities transactions, adjusted gross income, and information sufficient to calculate the purported effective federal income tax rates he paid for these years.

52. The IRS made these unlawful disclosures knowingly, or at the very least negligently or with gross negligence, including because the disclosures were made while willfully failing to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of Mr. Griffin's confidential taxpayer information from the unlawful disclosures alleged herein.

53. On information and belief, the IRS disclosed the confidential return information to ProPublica with the intent that ProPublica would widely publish the information through its website or through other means.

54. The IRS's disclosures of Mr. Griffin's tax return information did not result from a "good faith, but erroneous interpretation of section 6103,"[76] but rather from knowing violations, gross negligence, and/or negligence.

55. The IRS's disclosures of Mr. Griffin's tax return information to ProPublica was not "requested by the taxpayer," Mr. Griffin, pursuant to 26 U.S.C. § 7431(b)(2).

56. Separately, and in the alternative, as alleged herein, the IRS violated 26 U.S.C. § 6103 by disclosing confidential tax return information, in whole or in part, to certain IRS personnel (including Mr. Littlejohn) regardless of whether they completed or remained up to date with the all of the required IRS-provided privacy and data security training. Indeed, even if the

[76] 26 U.S.C. § 7431(b)(1).

disclosure of some of Mr. Griffin's confidential return information was necessary to perform Mr. Littlejohn's work for the IRS,[77] the disclosures still violated 26 U.S.C. § 6103 because IRS personnel disclosed Mr. Griffin's confidential tax return information to Mr. Littlejohn even though Mr. Littlejohn could have reasonably, properly, and economically performed his work for the IRS with only parts or portions of Mr. Griffin's confidential return information or, in the alternative, Mr. Littlejohn's work for the IRS would not have been seriously impaired if Mr. Griffin's taxpayer identity information were deleted from his returns prior to their disclosures to Mr. Littlejohn.[78]

57. The IRS's disclosure of Mr. Griffin's tax return information therefore violated 26 U.S.C. § 6103.

58. Pursuant to 26 U.S.C. § 7431, Mr. Griffin is entitled to statutory damages in the amount of $1,000 per each act of unauthorized disclosure.

59. Mr. Griffin is also entitled to punitive damages pursuant to 26 U.S.C. § 7431(c)(1)(B)(ii) because the IRS's unlawful disclosure of his confidential tax return information was either willful or a result of gross negligence.

60. Mr. Griffin is entitled to the costs of the action and reasonable attorney's fees pursuant to 26 U.S.C. § 7431(c)(3) if he is the prevailing party in this action.

---

[77] For example, pursuant to 26 U.S.C. § 6103(n).

[78] *See* 26 C.F.R. § 301.6103(n)-1(b)(2) ("Disclosure of returns or return information in connection with a written contract or agreement for the acquisition of property or services [pursuant to 26 U.S.C. § 6103(n)] shall be made only to the extent necessary to reasonably, properly, or economically perform the contract. If it is determined that disclosure of return or return information is necessary, and if the services can be reasonably, properly, or economically performed by disclosure of only parts or portions of a return or if deletion of taxpayer identity information […] reflected on a return would not seriously impair the ability of the employees to perform the service, then only the parts or portions of the return, or only the return with taxpayer identity information deleted, may be disclosed.").

COUNT II

Violation of 5 U.S.C. § 552a(e)(10) – The Privacy Act

61. Mr. Griffin realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

62. The IRS is an agency within the meaning of the Privacy Act.

63. The IRS maintained the records of Mr. Griffin, including his confidential tax return information, in a system of records as those terms are defined in the Privacy Act.

64. The IRS has long been aware of serious deficiencies in its safeguards, including as a result of repeated notice from TIGTA.

65. In violation of the Privacy Act, the IRS willfully and intentionally failed to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records, including Mr. Griffin's confidential tax return information, and failed to protect against any anticipated threats or hazards to those records' security or integrity, including those that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

66. The IRS also violated FISMA and provisions of the Internal Revenue Manual, as alleged herein, by failing to establish appropriate administrative, technical, and physical safeguards over its system of records.

67. As a direct and proximate result of its violations of the Privacy Act and FISMA, the IRS failed to take reasonable steps to prevent its personnel from unlawfully disclosing Mr. Griffin's records—his confidential tax return information—without his prior written consent and for no statutorily permitted purpose.

68. Mr. Griffin has and will continue to sustain damages directly traceable to the IRS's

violations set forth above. Mr. Griffin is therefore entitled to damages under 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

JURY DEMAND

Pursuant to Rule 38(a) of the Federal Rules of Civil Procedure, Plaintiff demands a trial by jury of all claims asserted in this Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Kenneth C. Griffin respectfully requests that the Court enter judgment in his favor and against Defendants as follows:

A. Declaring that the IRS willfully, knowingly, and/or by gross negligence, unlawfully disclosed Mr. Griffin's confidential tax return information in violation of 26 U.S.C. § 6103;

B. Declaring that the IRS willfully, knowingly, and/or by gross negligence, unlawfully inspected Mr. Griffin's confidential tax return information in violation of 26 U.S.C. § 6103;

C. Awarding Mr. Griffin $1,000 in damages for each unauthorized disclosure of his tax return information, including subsequent disclosure pursuant to 26 U.S.C. § 7431(c)(1);

D. Awarding Mr. Griffin reasonable costs and attorney's fees pursuant to 26 U.S.C. § 7431(c)(2)-(3) and as may otherwise be permitted by law;

E. Ordering Defendants to produce to Mr. Griffin all documents in their possession, custody, or control regarding the inspection, transmittal, and/or disclosure of Mr. Griffin's confidential tax return information to ProPublica;

F. Ordering the IRS to formulate, adopt, and implement a data security plan that

satisfies the requirements of the Privacy Act;

G. Awarding pre-and post-judgment interest as allowed by law; and

H. Any such other relief as the Court deems just and proper.

Dated: October 27, 2023

Respectfully submitted,

By: *Jason D. Sternberg*
William A. Burck (*pro hac vice*)
Derek L. Shaffer (*pro hac vice*)
Alexander J. Merton (*pro hac vice*)
QUINN EMANUEL URQUHART & SULLIVAN LLP
1300 I Street, N.W., Suite 900
Washington, DC 20005
(202) 538-8334
williamburck@quinnemanuel.com
derekshaffer@quinnemanuel.com
ajmerton@quinnemanuel.com

Christopher D. Kercher (*pro hac vice*)
Peter H. Fountain (*pro hac vice*)
QUINN EMANUEL URQUHART & SULLIVAN LLP
51 Madison Avenue, 22nd Floor,
New York, New York 10010
(212) 849-7000
christopherkercher@quinnemanuel.com
peterfountain@quinnemanuel.com

John F. Bash (*pro hac vice*)
QUINN EMANUEL URQUHART & SULLIVAN LLP
300 West 6th St, Suite 2010
Austin, TX 78701
(737) 667-6100
johnbash@quinnemanuel.com

Jason D. Sternberg
QUINN EMANUEL URQUHART & SULLIVAN LLP
2601 South Bayshore Drive, Suite 1550
Miami, FL 33133
(786) 850-3607
jasonsternberg@quinnemanuel.com

Counsel to Plaintiff Kenneth C. Griffin

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that, on this 27th day of October, 2023, I caused a copy of the foregoing document to be filed with the Clerk of Court using the CM/ECF electronic filing system, which will send notification to all counsel of record.

By: *Jason D. Sternberg*
Jason D. Sternberg
Fla. Bar No. 72887
jasonsternberg@quinnemanuel.com